



TITLE:

# Uniformly definable subrings of some infinite algebraic extensions of the rationals (New developments of independence notions in model theory)

AUTHOR(S):

Fukuzaki, Kenji

---

CITATION:

Fukuzaki, Kenji. Uniformly definable subrings of some infinite algebraic extensions of the rationals (New developments of independence notions in model theory). 数理解析研究所講究録 2010, 1718: 102-113

ISSUE DATE:

2010-10

URL:

<http://hdl.handle.net/2433/170340>

RIGHT:

# Uniformly definable subrings of some infinite algebraic extensions of the rationals

鹿児島国際大学国際文化学部 福崎賢治 (Kenji Fukuzaki)  
Faculty of Intercultural Studies,  
The international University of Kagoshima

## Abstract

We consider the formulas used by Julia Robinson in her proof that number fields are first order undecidable. We extend the result of [1]. We prove that it defines subrings in some infinite algebraic extensions of the rationals. As an application we discuss undecidabilities of those infinite algebraic extensions.

## 1 Introduction

In 1959 Julia Robinson [8] proved that any number field, as well as the corresponding ring of algebraic integers, is undecidable, by showing that  $\mathbb{N}$  is  $\emptyset$ -definable (in the ring language) in the ring, and the ring is  $\emptyset$ -definable in its number field.

She first considered the formula

$$\varphi_m(s, u, t) : \exists x, y, z (1 - sut^{2m} = x^2 - sy^2 - uz^2),$$

where  $m$  is a positive integer such that  $\mathfrak{p}^m \nmid 2$  for all prime ideals  $\mathfrak{p}$  of a given number field  $F$ , that is,  $m$  is an integer greater than all the ramification indices of prime ideals of  $F$  which divide 2. Then she proved that for a given prime  $\mathfrak{p}_1$  of  $F$  there are  $a, b \in F$  such that  $\varphi_m(a, b, t)$  defines a finite intersection of valuation rings  $\bigcap_{\mathfrak{p} \in \Delta} \mathcal{O}_{\mathfrak{p}}$  where  $\Delta$  is a finite set of primes of  $F$  containing  $\mathfrak{p}_1$ . (We actually can define the valuation ring of  $\mathfrak{p}_0$  using two  $\varphi_m(s, t, u)$  with some choice of those parameters. ) We denote by  $\varphi_m(a, b, F)$  the solution set of  $\varphi_m(a, b, t)$  in  $F$ , that is,  $\varphi_m(a, b, F) = \{\alpha \in F : F \models \varphi_m(a, b, \alpha)\}$ . It is easy to see that  $\bigcap_{a, b \in F} \varphi_m(a, b, F) = 0$ . Therefore in order to define the ring of algebraic integers  $\mathfrak{o}_F$  in a given number field  $F$ , J. Robinson considered the intersection of all  $\varphi_m(a, b, F)$  containing  $\mathbb{Z}$ , which is defined by  $\psi_m(t)$  :

$$\forall s, u (\forall c (\varphi_m(s, u, c) \rightarrow \varphi_m(s, u, c+1)) \rightarrow \varphi_m(s, u, t)).$$

Note that  $\varphi_m(s, u, t) \leftrightarrow \varphi_m(s, u, -t)$ . We denote by  $\psi_m(F)$  the solution set of  $\psi_m(t)$  in  $F$  as before. It is possible to define  $\mathfrak{o}_F$  since  $\mathbb{Z} \subseteq \psi_m(F) \subseteq \mathfrak{o}_F$  and  $F$  has an integral basis over the rationals  $\mathbb{Q}$ . (The defining formula of  $\mathfrak{o}_F$  depends on  $F$ . )

In this paper we calculate the solution set of  $\psi_2(t)$  in some infinite algebraic extensions of  $\mathbb{Q}$ .

## 2 Construction of $\psi(t)$

Let  $F$  be a number field (a finite algebraic extension of the rationals  $\mathbb{Q}$ ) and let  $\mathfrak{o}_F$  be the ring of algebraic integers of  $F$ .  $F^*$  will denote the set of non-zero elements of  $F$ . By  $\mathfrak{p}$  we denote a place of  $F$  and by  $F_{\mathfrak{p}}$  the completion of  $F$  with respect to  $\mathfrak{p}$ . Since non-archimedean places of  $F$  are  $\mathfrak{p}$ -adic valuations for some prime ideal  $\mathfrak{p}$  of  $F$ , we use the same letter  $\mathfrak{p}$  for both the place and the prime ideal. The ring of integers of  $F_{\mathfrak{p}}$  is denoted by  $(\mathfrak{o}_F)_{\mathfrak{p}}$ , its maximal ideal is also denoted by  $\mathfrak{p}$ . Let  $\mathfrak{p}$  be a prime ideal of  $F$  and  $a \in F$ . By  $\nu_{\mathfrak{p}}(a)$  we denote the order of  $a$  at  $\mathfrak{p}$ . Given  $a, b \in F^*$ , we use Hilbert symbol  $(a, b)_{\mathfrak{p}}$ , which is defined to be  $+1$  if  $ax^2 + by^2 = 1$  is solvable in  $F_{\mathfrak{p}}$ , otherwise defined to be  $-1$ . For  $a, b \in F^*$  we denote by  $S_F(a, b)$  the set of places  $\mathfrak{p}$  of  $F$  such that  $(a, b)_{\mathfrak{p}} = -1$ . We know that it contains even number of places of  $F$ .

The following lemma is well-known.

**Lemma 1** *A nonzero element  $h$  of  $F$  can be represented by the ternary quadratic form  $x^2 - ay^2 - bz^2$  in  $F$  if and only if  $h/(-ab) \notin F_{\mathfrak{p}}^{*2}$  for any place  $\mathfrak{p}$  such that  $(a, b)_{\mathfrak{p}} = -1$ .*

This follows from the properties of quaternary quadratic forms and the Hasse-Minkowski theorem on quadratic forms. See [7, p. 187].

**Lemma 2** *Given even number of distinct prime ideals  $\mathfrak{p}_1, \dots, \mathfrak{p}_{2k}$  of  $F$  there are  $a$  and  $b$  in  $F^*$  such that  $S_F(a, b) = \{\mathfrak{p}_1, \dots, \mathfrak{p}_{2k}\}$  and  $\nu_{\mathfrak{p}_i}(a) = 1$ ,  $\nu_{\mathfrak{p}_i}(b) = 0$  for  $i = 1, \dots, 2k$ .*

*Proof.* By weak approximation, we get an element  $a$  of  $F^*$  with  $\nu_{\mathfrak{p}_i}(a) = 1$  for all  $i$ . We know by [7, 71:19. Theorem p. 203] that there is  $b \in F^*$  such that  $S_F(a, b) = \{\mathfrak{p}_1, \dots, \mathfrak{p}_{2k}\}$ . In the proof of [7, 71:19. Theorem p. 203], we can take  $b$  with  $\nu_{\mathfrak{p}_i}(b) = 0$  for  $i = 1, \dots, 2k$ .  $\square$

J. Robinson actually proved in [8, Lemma 9] that given a prime ideal  $\mathfrak{p}_1$  of  $F$  there are relatively prime elements  $a$  and  $b$  in  $\mathfrak{o}_F$  such that  $(a) = \mathfrak{p}_1 \cdots \mathfrak{p}_{2k}$ , where  $\mathfrak{p}_1, \dots, \mathfrak{p}_{2k}$  are distinct prime ideals that include every prime ideal dividing 2, and  $b$  is a totally positive prime element such that  $(a, b)_{\mathfrak{p}} = -1$  iff  $\mathfrak{p} | a$ .

**Lemma 3** *Let  $a, b, c \in F$ . If  $a$  and  $b$  satisfy Lemma 2 and  $m$  be a positive integer such that  $\mathfrak{p}^m \nmid 2$  for every prime ideal  $\mathfrak{p}$ . Then*

*$1 - abc^{2m} = x^2 - ay^2 - bz^2$  is solvable for  $x, y$  and  $z$  in  $F$  iff  $\nu_{\mathfrak{p}_i}(c) \geq 0$  for each  $i$ .*

*Proof.* By Lemma 1,  $h = 1 - abc^{2m}$  can be represented by  $x^2 - ay^2 - bz^2$  iff  $h/(-ab) \notin F_{\mathfrak{p}_i}^{*2}$  for  $1 \leq i \leq 2k$ .

If  $\nu_{\mathfrak{p}_i}(c) \geq 0$  for each  $i$ , then we have  $\nu_{\mathfrak{p}_i}(h/(-ab)) = -1$ , hence  $h/(-ab)$  is not a square of  $F_{\mathfrak{p}_i}$  for each  $i$ .

Suppose  $\nu_{\mathfrak{p}_i}(c) < 0$  for some  $i$ . We know in  $F_{\mathfrak{p}}$  that  $(1 + \mathfrak{p}^r)^2 = 1 + 2\mathfrak{p}^r$  if  $\mathfrak{p}^r \subseteq 2\mathfrak{p}$  by [7, p. 163]. Noting  $h/(-ab) = c^{2m}(1 - 1/(abc^{2m}))$ , we see that  $h/(-ab)$  is a square of  $F_{\mathfrak{p}_i}$  since  $\nu_{\mathfrak{p}_i}(1/(abc^{2m})) \geq 2m - 1$  and  $\mathfrak{p}^{2m-1} \subseteq 2\mathfrak{p}$ .  $\square$

Thus we have that if  $a$  and  $b$  satisfy Lemma 2,  $\varphi_m(a, b, F) = \bigcap_{1 \leq i \leq 2k} \mathcal{O}_{\mathfrak{p}_i}$ , and  $\forall c(\varphi_m(a, b, c) \rightarrow \varphi_m(a, b, c + 1))$  holds in  $F$  since  $\varphi_m(a, b, F)$  is a ring containing  $\mathbb{Z}$ .

For a given  $c \in F^*$  there are  $a, b \in F^*$  such that  $c \notin \varphi_m(a, b, F)$  since we can construct  $a, b \in F^*$  such that  $1 - 1/(abc^{2m})$  is a square of  $F_{\mathfrak{p}}$  for some  $\mathfrak{p}$  with  $(a, b)_{\mathfrak{p}} = -1$ . Noting  $0 \in \varphi_m(a, b, F)$  for all  $a, b$  we have  $\bigcap_{a, b \in F} \varphi_m(a, b, F) = 0$ .

Nevertheless we have that  $\psi_m(F)$  is a subset of  $\mathfrak{o}_F$  containing  $\mathbb{Z}$  since  $\psi_m(F)$  is the intersection of all the solution set of

$$\forall c(\varphi_m(a, b, c) \rightarrow \varphi_m(a, b, c + 1)) \rightarrow \varphi_m(a, b, t).$$

If the premise of the above formula fails, the solution set is  $F$ .

We don't know what  $\psi_m(F)$  is. But we can show what  $\psi_2(K)$  is, if  $K$  is a certain infinite algebraic extension of  $\mathbb{Q}$ .

**Remark 4** For a given prime ideal  $\mathfrak{p}_1$  we can define the valuation ring of  $\mathfrak{p}_1$ . Take three prime ideal  $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$  of  $F$  and  $a, b, c, d \in \mathfrak{o}_F$  such that  $S_F(a, b) = \{\mathfrak{p}_1, \mathfrak{p}_2\}$  and  $S_F(c, d) = \{\mathfrak{p}_1, \mathfrak{p}_3\}$ , then we easily see that  $\varphi_m(a, b, F) + \varphi_m(c, d, F)$  defines  $\mathcal{O}_{\mathfrak{p}_1}$ .

### 3 The solution set of $\psi(t)$ in some infinite algebraic extensions

Let  $F$  be a number field and let  $\mathcal{F}$  be an infinite set of finite Galois extensions  $M$  of  $F$  such that  $[M : F]$  is odd and every prime ideal of  $M$  dividing 2 is unramified in  $M/\mathbb{Q}$ . (We say that 2 is unramified in  $M/\mathbb{Q}$ . Note  $\mathfrak{p}^2 \nmid 2$  for all prime ideals  $\mathfrak{p}$  of  $M$ .) Let  $K$  be the composite field of all fields in  $\mathcal{F}$ . Then  $K$  is an infinite Galois extension of  $F$  and every finite Galois subextension  $M$  has odd extension degree over  $\mathbb{Q}$ . We denote by  $\mathfrak{O}_K$  the ring of algebraic integers of  $K$ .

In this section we will prove that the solution set  $\psi_2(K)$  of  $\psi_2(t)$  in  $K$  is a subset of  $\mathfrak{O}_K$  containing  $\mathbb{Z}$ .

We need the following lemma, which is proved in [2, pp. 272, 337].

**Lemma 5** *Let  $M, L$  be number fields with  $L \supset M$  and let  $\mathfrak{P} \supset \mathfrak{p}$  be primes of  $L$  and  $M$  respectively. For  $\alpha \in L_{\mathfrak{P}}^*$ , let  $a = N_{L_{\mathfrak{P}}/M_{\mathfrak{p}}}(\alpha)$  and  $b \in M_{\mathfrak{p}}$ . Then we have  $(\alpha, b)_{\mathfrak{P}} = (a, b)_{\mathfrak{p}}$ .*

The next lemma follows from Lemma 5.

**Lemma 6** *Let  $L$  be a finite Galois extension of a number field  $M$  with  $[L : M]$  odd. Let  $\mathfrak{p}$  be a prime ideal of  $M$  and let  $\mathfrak{P}$  be a prime of  $L$  lying over  $\mathfrak{p}$ . Then for  $a, b \in M^*$ , we have  $(a, b)_{\mathfrak{p}} = 1$  iff  $(a, b)_{\mathfrak{P}} = 1$ .*

*Proof.* Since  $L/M$  is a Galois extension, the local degree at  $\mathfrak{P}$  divides the degree of  $L/M$ , that is,  $[(L)_{\mathfrak{P}} : (M)_{\mathfrak{p}}] \mid [L : M]$  (see [7, p. 32]). Let  $u$  be the local degree at  $\mathfrak{P}$ . Then  $N_{(L)_{\mathfrak{P}}/(M)_{\mathfrak{p}}}(a) = a^u$  and  $(a, b)_{\mathfrak{P}} = (a^u, b)_{\mathfrak{p}} = (a, b)_{\mathfrak{p}}^u$ . Since  $u$  is odd, it follows that  $(a, b)_{\mathfrak{p}} = 1$  iff  $(a, b)_{\mathfrak{P}} = 1$ .  $\square$

We recall that  $\varphi_2(s, u, t)$  is

$$\exists x, y, z(1 - sut^4 = x^2 - sy^2 - uz^2)$$

and  $\psi_2(t)$  is

$$\forall s, u(\forall c(\varphi(s, u, c) \rightarrow \varphi(s, u, c+1)) \rightarrow \varphi_2(s, u, t)).$$

**Lemma 7** *Let  $M$  be a subfield of  $K$  with  $M/F$  finite and Galois. Let  $a, b, \alpha \in M$  with  $ab \neq 0$ . Then*

$$M \models \varphi(a, b, \alpha) \text{ iff } K \models \varphi(a, b, \alpha).$$

*Proof.* If  $M \models \varphi(a, b, \alpha)$ , then we have trivially  $K \models \varphi(a, b, \alpha)$ .

If  $M \models \neg\varphi(a, b, \alpha)$ , then  $(1 - ab\alpha^4)/(-ab) \in M_{\mathfrak{p}}^{*2}$  for some  $\mathfrak{p}$  a place of  $M$  such that  $(a, b)_{\mathfrak{p}} = -1$ . Let  $L$  be any subfield of  $K$  with  $L/M$  finite and Galois and let  $\mathfrak{P}$  be a place of  $M$  lying above  $\mathfrak{p}$ . Since  $[L : M]$  is odd we have  $(a, b)_{\mathfrak{P}} = -1$  and  $(1 - ab\alpha^4)/(-ab) \in L_{\mathfrak{P}}^{*2}$ . Hence  $L \models \neg\varphi(a, b, \alpha)$  and  $K \models \neg\varphi(a, b, \alpha)$ . Note that for archimedean places  $\mathfrak{p} \subset \mathfrak{P}$ , it is also true that  $(a, b)_{\mathfrak{p}} = 1$  iff  $(a, b)_{\mathfrak{P}} = 1$ .  $\square$

**Theorem 8** *The solution set  $\psi_2(K)$  of  $\psi_2(t)$  in  $K$  is a subset of  $\mathfrak{D}_K$  containing  $\mathbb{Z}$  ( $\mathbb{Z} \subseteq \psi_2(K) \subseteq \mathfrak{D}_K$ ).*

*Proof.* We have trivially  $\mathbb{Z} \subseteq \psi_2(K)$ . Let  $t \in K \setminus \mathfrak{D}_K$ . We show that there are  $a, b \in K$  such that

$$K \models \neg\varphi_2(a, b, t) \wedge \forall c(\varphi_2(a, b, c) \rightarrow \varphi_2(a, b, c+1)).$$

We fix a subfield  $M$  of  $K$  such that  $[M : F]$  is finite and  $t \in M$ . Then we have  $\nu_{\mathfrak{p}_1}(t) < 0$  for some prime  $\mathfrak{p}_1$  of  $M$ . Take a prime  $\mathfrak{p}_2 \neq \mathfrak{p}_1$  of  $M$ . By Lemma 2, there are  $a$  and  $b$  in  $M^*$  such that  $\nu_{\mathfrak{p}_1}(a) = 1$ ,  $\nu_{\mathfrak{p}_1}(b) = 0$  and  $(a, b)_{\mathfrak{p}_i} = -1$  for  $i = 1, 2$ , and  $t \notin \varphi_2(a, b, M)$ . By Lemma 7,  $1 - abt^4 = x^2 - ay^2 - bz^2$  is not solvable for  $x, y, z$  in  $K$ .

Let  $c$  in  $K$  and suppose  $K \models \varphi_2(a, b, c)$ . Take a subfield  $L$  of  $K$  such that  $L$  contains  $c$  and  $L/M$  is a finite Galois extension, then we have  $L \models \varphi_2(a, b, c)$  by

Lemma 7. Let  $h = 1 - abc^4$  and  $h' = 1 - ab(c+1)^4$ . Let  $\mathfrak{P}_1, \dots, \mathfrak{P}_k$  be all the primes of  $L$  lying above  $\mathfrak{p}_1$  and  $\mathfrak{P}_{k+1}, \dots, \mathfrak{P}_{k+s}$  be all the primes of  $L$  lying above  $\mathfrak{p}_2$ . By Lemma 5, we have  $S_L(a, b) = \{\mathfrak{P}_1, \dots, \mathfrak{P}_{k+s}\}$ , that is,  $\mathfrak{P}_i$  are all the primes  $\mathfrak{P}$  of  $L$  such that  $(a, b)_{\mathfrak{P}} = -1$ .  $k$  and  $s$  are odd since  $L/M$  is Galois with odd extension degree. We will show that for all  $\mathfrak{P}_i$ ,  $h'/(-ab)$  is not a square of  $L^{\mathfrak{P}_i}$ , assuming  $h/(-ab)$  is not. Take one  $\mathfrak{P} = \mathfrak{P}_i$ . We will break into cases according to whether or not  $\mathfrak{P}$  divides 2.

Case 1:  $\mathfrak{P} \nmid 2$ .

As mentioned before we have  $(1 + \mathfrak{p}^r)^2 = 1 + 2\mathfrak{p}^r$  if  $\mathfrak{p}^r \subseteq 2\mathfrak{p}$  by [7, p. 163]. Hence we have  $(1 + \mathfrak{P})^2 = 1 + \mathfrak{P}$ . If  $\nu_{\mathfrak{P}}(c) \geq 0$ , then  $h' = 1 - ab(c+1)^4$  is a square of  $L_{\mathfrak{P}}$  since  $\nu_{\mathfrak{P}}(-ab(c+1)^4) > 0$ . Since  $(a, b)_{\mathfrak{P}} = (a, -ab)_{\mathfrak{P}} = -1$  we have  $-ab$  is not a square of  $L_{\mathfrak{P}}$ , hence  $h'/(-ab)$  is also not.

We consider the case  $\nu_{\mathfrak{P}}(c) < 0$ . Since  $h/(-ab) = c^4(1 - 1/(abc^4))$  it follows that  $\nu_{\mathfrak{P}}(-abc^4) \geq 0$ . Let  $\mathfrak{P}$  lie above  $\mathfrak{p}_i$  and let  $e = e(\mathfrak{P}/\mathfrak{p}_i)$  be the ramification index of  $\mathfrak{P}$ .  $e$  must be odd since  $L/M$  is Galois with odd extension degree. Hence we have  $\nu_{\mathfrak{P}}(-abc^4) > 0$ . Then we have  $\nu_{\mathfrak{P}}(-ab(c+1)^4) = \nu_{\mathfrak{P}}(-ab) + 4\nu_{\mathfrak{P}}(c) = \nu_{\mathfrak{P}}(-abc^4) > 0$ , hence  $h' = 1 - ab(c+1)^4$  is a square of  $L_{\mathfrak{P}}$  and  $h'/(-ab)$  is not.

Case 2:  $\mathfrak{P} | 2$ .

Since 2 is unramified in  $L/\mathbb{Q}$  we have  $\nu_{\mathfrak{P}}(2) = 1$  and  $\nu_{\mathfrak{P}}(-ab) = 1$ . Furthermore we know  $(1 + \mathfrak{P})^2 = 1 + \mathfrak{P}^3$  by [7, p. 163]. If  $\nu_{\mathfrak{P}}(c) < 0$  then  $h'/(-ab) = c^4(1 - 1/(abc^4))$  would be a square of  $L^{\mathfrak{P}}$ , hence we have  $\nu_{\mathfrak{P}}(c) \geq 0$ . It follows that  $\nu_{\mathfrak{P}}(h'/(-ab)) = -1$  and  $h'/(-ab)$  is not a square of  $L_{\mathfrak{P}}$ .  $\square$

**Example 9** 1. Let  $F = \mathbb{Q}((\zeta_l))$  and  $\mathcal{F}$  be a set of all  $M_n = \mathbb{Q}(\zeta_{l^n})$  ( $n > 1$ ), where  $l$  is an odd integer  $> 1$  and  $\zeta_{l^n}$  is a primitive  $l^n$ -th root of unity.  $K = \bigcup_n M_n$ .

2. Let  $F = \mathbb{Q}$  and  $\mathcal{F}$  be a set of all  $\mathbb{Q}(\cos(2\pi/l^n))$ , where  $n \in \mathbb{N}$  and  $l$  is an odd prime with  $l \equiv -1 \pmod{4}$ .  $K = \mathbb{Q}(\{\cos(2\pi/l^n) : n \in \mathbb{N}, l \text{ a prime}, l \equiv -1 \pmod{4}\})$ .

**Remark 10** In the proof of Theorem 8, we have  $\varphi_2(a, b, M) = \mathcal{O}_{\mathfrak{p}_1}^M \cap \mathcal{O}_{\mathfrak{p}_2}^M$ . Here  $\mathcal{O}_{\mathfrak{p}_i}^M$  denotes the valuation ring of  $\mathfrak{p}_i$  in  $M$ . But it is not necessarily true that  $\varphi_2(a, b, L) = \bigcap_i \mathcal{O}_{\mathfrak{p}_i}^L$ . Actually we have  $\varphi_2(a, b, M) \subseteq \bigcap_i \mathcal{O}_{\mathfrak{p}_i}^L \subseteq \varphi_2(a, b, L)$ .

Nevertheless we can prove  $\varphi_2(a, b, L) = \bigcap_i \mathcal{O}_{\mathfrak{p}_i}^L$  for  $K = \bigcup_n \mathbb{Q}(\zeta_{l^n})$ , where  $l$  is an odd prime and  $\zeta_{l^n}$  is a primitive  $l^n$ -th root of unity.

## 4 The structure of $\psi(K)$

In this section we let  $F = \mathbb{Q}$ , that is, let  $K$  be the composite of all fields in  $\mathcal{F}_0$  where  $\mathcal{F}_0$  is a set of infinitely many finite Galois extensions  $M$  of  $\mathbb{Q}$  such that  $[M : \mathbb{Q}]$  is odd

and 2 is unramified in  $M/\mathbb{Q}$ . We let  $\mathcal{F}$  be the family of all finite Galois subextensions of  $K$ . Then every  $M$  also has odd extension degree over  $\mathbb{Q}$  and 2 is unramified in  $M/\mathbb{Q}$ . We write  $\varphi$  and  $\psi$  instead of  $\varphi_2$  and  $\psi_2$  respectively.

We shall investigate what  $\psi(K)$  is. For  $a, b \in K$  we let  $T_{a,b}$  be the set of elements  $\alpha$  of  $K$  such that

$$K \models \forall c(\varphi(a, b, c) \rightarrow \varphi(a, b, c+1)) \rightarrow \varphi(a, b, \alpha).$$

Then we have  $\psi(\mathfrak{O}_K) = \bigcap_{a,b \in K} T_{a,b}$ . We easily see  $T_{a,b} = K$  for  $a, b$  with  $ab = 0$ . So we shall investigate what  $T_{a,b}$  is, for  $a, b \in K^*$ . We recall that for  $a, b \in M^*$ ,  $M \models \neg\varphi(a, b, \alpha)$  iff  $\alpha^4 - 1/ab \in M_{\mathfrak{p}}^{*2}$  for some  $\mathfrak{p} \in S_M(a, b)$ . Hence we easily see the following: for  $a, b \in K^*$ , if  $S_M(a, b) = \emptyset$  for some  $M \in \mathcal{F}$  with  $a, b \in M$ , then  $\varphi(a, b, K) = T_{a,b} = K$  by Lemma 6. So we shall investigate what  $T_{a,b}$  is, for  $a, b \in K^*$  such that for some  $M \in \mathcal{F}$  with  $a, b \in M$ ,  $S_M(a, b) \neq \emptyset$ .

From now on we use the following notation. For a number field  $M$ , the ring of integers of  $M_{\mathfrak{p}}$  is denoted by  $(\mathfrak{o}_M)_{\mathfrak{p}}$ , its maximal ideal is also denoted by  $\mathfrak{p}$ , its residue field  $(\mathfrak{o}_M)_{\mathfrak{p}}/\mathfrak{p}$  by  $(\bar{M})_{\mathfrak{p}}$ , and the group of units of  $(\mathfrak{o}_M)_{\mathfrak{p}}$  by  $(U_M)_{\mathfrak{p}}$ . For  $\alpha \in \mathcal{M}$ , we denote by  $\bar{\alpha}$  its residue class in  $(\bar{M})_{\mathfrak{p}}$ . Furthermore we usually let  $\mathfrak{p}$  lie above a rational prime  $p$ . Note that  $(\bar{M})_{\mathfrak{p}} \simeq \mathfrak{o}_M/\mathfrak{p} \simeq \mathbb{F}_{p^f}$  where  $f$  is the residue degree of  $M$  at  $\mathfrak{p}$ .

**Lemma 11** *Let  $a, b \in K^*$  such that*

$$K \models \forall c(\varphi(a, b, c) \rightarrow \varphi(a, b, c+1))$$

*holds. Then for every  $M \in \mathcal{F}$  with  $a, b \in M$ , every  $\mathfrak{p} \in S_M(a, b)$  is not archimedean.*

This is proved similarly as Lemma 14 in [1].

**Lemma 12** *Let  $M \in \mathcal{F}$ . Let  $a, b \in M^*$ ,  $\alpha \in \mathfrak{o}_M$  and  $\mathfrak{p}_0 \in S_M(a, b)$  with  $\mathfrak{p}_0 \nmid 2$  such that*

1.  $K \models \forall c(\varphi(a, b, c) \rightarrow \varphi(a, b, c+1))$  and
2.  $\alpha^4 - 1/ab \in M_{\mathfrak{p}_0}^{*2}$  hold.

*Then  $\nu_{\mathfrak{p}_0}(-ab) = 0$  and  $\nu_{\mathfrak{p}_0}(\alpha) = 0$ .*

This is also proved similarly as Lemma 15 in [1].

Now we will prove the following lemma on finite fields.

**Lemma 13** *Let  $p$  be an odd prime and  $q = p^f$ . Let  $\mathbb{F}_q$  be a finite field with  $q$  elements other than  $\mathbb{F}_3, \mathbb{F}_5$ . We let  $\eta$  be the quadratic character of  $\mathbb{F}_q$ , that is,  $\eta(0) = 0, \eta(c) = 1$  if  $c \in \mathbb{F}_q^{*2}$  and  $\eta(c) = -1$  otherwise.*

*Then for all  $a \in \mathbb{F}_q^*$  with  $\eta(a) = -1$ ,*

*(†) there are  $b \in \mathbb{F}_q$  and  $j \in \mathbb{F}_p$  such that  $\eta(b^4 + a)\eta((b+j)^4 + a) = -1$ .*

*Exceptional cases are,  $\mathbb{F}_3$  and  $a = 2$ , and,  $\mathbb{F}_5$  and  $a = 2$ .*

*Proof.* We will first prove the following; for all  $a \in \mathbb{F}_q^*$  with sufficiently large  $q$ , we can take  $j = 1$  in the statement  $(\dagger)$ . We use Weil's Theorem [5, p. 225, Theorem 5.41], from which we have that for  $a \in \mathbb{F}_q^*$ ,

$$\left| \sum_{c \in \mathbb{F}_q} \eta\{(c^4 + a)((c+1)^4 + a)\} \right| \leq 7q^{1/2}.$$

Thus if  $q$  satisfies inequality  $7q^{1/2} < q - 8$  then for all  $a \in \mathbb{F}_q^*$  there is  $b \in \mathbb{F}_q$  such that  $\eta(b^4 + a)\eta((b+1)^4 + a) = -1$ . Hence for all  $\mathbb{F}_q$  with  $q > 64$  the assertion holds. For the small values of  $q \leq 64$  we can check the assertion directly.  $\square$

Note that in the statement  $(\dagger)$  we cannot always take  $j = 1$  if  $q \leq 64$ ; for example in  $\mathbb{F}_7$  there is no  $b$  such that  $\eta(b^4 + 5)\eta((b+1)^4 + 5) = -1$  but in  $\mathbb{F}_7$   $\eta(1^4 + 5)\eta((1+2)^4 + 5) = -1$  holds. Note also that we need the assumption  $\eta(a) = -1$  for  $\mathbb{F}_9$  since for  $a = 1, 2$ , for which  $\eta(a) = 1$ , the statement  $(\dagger)$  does not hold.

**Lemma 14** *Let  $M \in \mathcal{F}$ . Let  $a, b \in M^*$ . Suppose that  $S_M(a, b)$  contains a non-archimedean place  $\mathfrak{p}_0$  such that  $\mathfrak{p}_0 \nmid 2$ ,  $\nu_{\mathfrak{p}_0}(-ab) = 0$  and  $(\bar{M})_{\mathfrak{p}_0} \neq \mathbb{F}_3, \mathcal{F}_5$ .*

*Then  $K \models \neg \forall c(\varphi(a, b, c) \rightarrow \varphi(a, b, c+1))$ .*

The proof is similar to that of Lemma 16 in [1].

**Proposition 15** *Let  $M \in \mathcal{F}$ . For  $a, b \in M^*$ , if  $S_M(a, b)$  contains no primes dividing 2, then we have  $\mathfrak{O}_K \subseteq T_{a,b}$ , that is,*

$$K \models \forall c(\varphi(a, b, c) \rightarrow \varphi(a, b, c+1)) \rightarrow \varphi(a, b, \alpha) \text{ for all } \alpha \in \mathfrak{O}_{K_l}.$$

*Proof.* We first note the following; if we take  $N \in \mathcal{F}$  such that  $a, b \in N^*$  then  $S_N(a, b)$  also contains no primes dividing 2 by Lemma 6. Suppose not. Then there is  $\alpha \in \mathfrak{O}_K$  such that

$$K \models \forall c(\varphi(a, b, c) \rightarrow \varphi(a, b, c+1)) \text{ but } K_l \models \neg \varphi(a, b, \alpha).$$

Take  $N \in \mathcal{F}$  such that  $a, b, \alpha \in N$ . We have by Lemma 7,

$$N \models \forall c(\varphi(a, b, c) \rightarrow \varphi(a, b, c+1)) \text{ but } N \models \neg \varphi(a, b, \alpha).$$

Then there is a  $\mathfrak{p}_0 \in S_N(a, b)$  such that  $\alpha^4 - 1/ab \in N_{\mathfrak{p}_0}^{*2}$ .

We see that  $\mathfrak{p}_0$  is not archimedean by Lemma 11 and that  $\nu_{\mathfrak{p}_0}(-ab) = 0$  and  $\nu_{\mathfrak{p}_0}(\alpha) = 0$  by Lemma 12. If  $(\bar{N})_{\mathfrak{p}_0} \neq \mathbb{F}_3, \mathcal{F}_5$ , we get a contradiction by Lemma 14.

Suppose that  $(\bar{N})_{\mathfrak{p}_0} = \mathcal{F}_5$ . Since  $(a, b)_{\mathfrak{p}_0} = -1$  and  $N \models \psi(1)$ , we have  $-1/ab \in N_{\mathfrak{p}_0}^{*2}$  and  $1 - 1/ab \in N_{\mathfrak{p}_0}^{*2}$ , hence  $-1/ab \equiv 2 \pmod{\mathfrak{p}_0}$ . Since  $\nu_{\mathfrak{p}_0}(\alpha) = 0$ , we have



$\alpha^4 \equiv 1 \pmod{\mathfrak{p}_0}$ . Then we have  $\alpha^4 - 1/ab \equiv 3 \pmod{\mathfrak{p}_0}$ , hence  $\alpha^4 - 1/ab \notin N_{\mathfrak{p}_0}^{*2}$ , a contradiction.

Suppose that  $(\bar{N})_{\mathfrak{p}_0} = \mathcal{F}_3$ . We first deal with the case where  $\mathfrak{p}_0$  is not ramified in  $N/\mathbb{Q}$ . Then 3 is a prime element of  $N_{\mathfrak{p}_0}$  and we can write  $-1/ab = 2 + s_1 3 + s_2 3^2 + \dots$ , where  $s_i \in \{0, 1, 2\}$ . We note that  $N \models \varphi(a, b, n)$  for all  $n \in \mathbb{N}$ . If  $s_1 = 0$ , then  $2^4 - 1/ab = (s_2 + 2)3^2 + \dots$ ,  $7^4 - 1/ab = s_2 3^2 + \dots$  and  $11^4 - 1/ab = (s_2 + 1)3^2 + \dots$ . Thus we have one of these three must be contained in  $N_{\mathfrak{p}_0}^{*2}$ , a contradiction. Likewise if  $s_1 = 1$ , then  $4^4 - 1/ab = (s_2 + 2)3^2 + \dots$ ,  $13^4 - 1/ab = s_2 3^2 + \dots$  and  $5^4 - 1/ab = (s_2 + 1)3^2 + \dots$ . And if  $s_1 = 2$ , then  $1^4 - 1/ab = (s_2 + 1)3^2 + \dots$ ,  $8^4 - 1/ab = s_2 3^2 + \dots$  and  $10^4 - 1/ab = (s_2 + 1)3^2 + \dots$ . Thus in the case where  $\mathfrak{p}_0$  is not ramified in  $N/\mathbb{Q}$ , we get contradictions.

Secondly We deal with the case where  $\mathfrak{p}_0$  is ramified in  $N/\mathbb{Q}$ . Let  $\nu_{\mathfrak{p}_0}(3) = e$  and let  $\pi$  be a prime element of  $N_{\mathfrak{p}_0}$ . We can write  $-1/ab = 2 + s_1 \pi + s_2 \pi^2 + \dots$ , where  $s_i \in \{0, 1, 2\}$ . We may write  $\alpha = 1 + c_1 \pi + c_2 \pi^2 + \dots$  where  $c_i \in \{0, 1, 2\}$ , since if  $\alpha \equiv 2 \pmod{\mathfrak{p}_0}$  then  $-\alpha \equiv 1 \pmod{\mathfrak{p}_0}$ . Since  $N \models \neg \varphi(a, b, \alpha)$ , we have  $N \models \neg \varphi(a, b, \alpha - n)$  for all  $n \in \mathbb{N}$ . But  $(\alpha - 1)^4 - 1/ab \equiv 2 \pmod{\mathfrak{p}_0}$ , hence there must be another prime  $\mathfrak{p}_1 \in S_N(a, b)$  with  $(\alpha - 1)^4 - 1/ab \in N_{\mathfrak{p}_1}^{*2}$ .  $\mathfrak{p}_1$  must be a prime lying above 3 and  $\alpha \equiv 2 \pmod{\mathfrak{p}_1}$ . And we have  $(\alpha - (3k + 1))^4 - 1/ab \equiv 2 \pmod{\mathfrak{p}_0}$  and  $(\alpha - (3k + 2))^4 - 1/ab \equiv 0 \pmod{\mathfrak{p}_0}$ . Likewise  $(\alpha - (3k + 1))^4 - 1/ab \equiv 0 \pmod{\mathfrak{p}_1}$  and  $(\alpha - (3k + 2))^4 - 1/ab \equiv 2 \pmod{\mathfrak{p}_1}$ . Since there are finitely many primes in  $S_N(a, b)$ , we must have for some  $k$   $(\alpha - (3k + 2))^4 - 1/ab \equiv 0 \pmod{\mathfrak{p}_0}$  and  $(\alpha - (3k + 2))^4 - 1/ab \in N_{\mathfrak{p}_0}^{*2}$ .

We have  $s_1 + c_1 \equiv 0 \pmod{\mathfrak{p}_0}$  since  $\alpha^4 - 1/ab = (s_1 - c_1)\pi + \dots$ . And we have  $s_1 - c_1 \equiv 0 \pmod{\mathfrak{p}_0}$  since  $(\alpha - (3k + 2))^4 - 1/ab = (s_1 - c_1)\pi + \dots$ . Thus we have  $s_1 \equiv 0 \pmod{\mathfrak{p}_0}$  and  $c_1 \equiv 0 \pmod{\mathfrak{p}_0}$ . Likewise we have  $s_2 \equiv 0 \pmod{\mathfrak{p}_0}$  and  $c_2 \equiv 0 \pmod{\mathfrak{p}_0}$ . We can proceed to  $\pi^{e-1}$ . It follows that  $-1/ab = 2 + s_e \pi^e + s_{e+1} \pi^{e+1} + \dots$ . Then we have  $2^4 - 1/ab = (s_e + 2)3^2 + \dots$ ,  $7^4 - 1/ab = s_e 3^2 + \dots$  and  $11^4 - 1/ab = (s_e + 1)3^2 + \dots$ , a contradiction.  $\square$

We will deal with primes dividing 2.

**Lemma 16** *Let  $M \in \mathcal{F}$ . Let  $a, b \in M^*$ ,  $\alpha \in \mathfrak{o}_M$  and  $\mathfrak{p}_0 \in S_M(a, b)$  with  $\mathfrak{p}_0 | 2$  such that*

1.  $K \models \forall c(\varphi(a, b, c) \rightarrow \varphi(a, b, c + 1))$  and
2.  $\alpha^4 - 1/ab \in M_{\mathfrak{p}_0}^{*2}$  hold.

*Then  $\nu_{\mathfrak{p}_0}(-ab) = \pm 2$ .*

The proof is similar to that of Lemma 18 in [1].

We shall prove a similar result to Lemma 14.

**Lemma 17** *Let  $M \in \mathcal{F}$  and  $a, b \in M^*$ . Suppose that  $S_n(a, b)$  contains a  $\mathfrak{p}_0$  such that  $\mathfrak{p}_0 | 2$  and  $\nu_{\mathfrak{p}_0}(-ab) = -2$ .*

*Then  $K_l \models \neg \forall c(\varphi(a, b, c) \rightarrow \varphi(a, b, c+1))$ .*

The proof is similar to that of Lemma 19 in [1]

Thus we get the following proposition. The proof is similar to that of Proposition 15.

**Proposition 18** *Let  $l$  be an odd prime such that  $l \equiv -1 \pmod{4}$ . For  $a, b \in F_n^*$ , if  $S_n(a, b)$  contains no primes  $\mathfrak{p}$  such that  $\mathfrak{p} | 2$  and  $\nu_{\mathfrak{p}}(-ab) = 2$ , then we have  $\mathfrak{O}_{K_l} \subseteq T_{a,b}$ , that is,*

$$K_l \models \forall c(\varphi(a, b, c) \rightarrow \varphi(a, b, c+1)) \rightarrow \varphi(a, b, \alpha) \text{ for all } \alpha \in \mathfrak{O}_{K_l}.$$

Since  $\psi(K) = \bigcap_{a,b \in K^*} T_{a,b} \subseteq \mathfrak{O}_K$ , Proposition 18 implies  $\psi(K) = \bigcap_{(a,b) \in \Delta} T_{a,b}$ , where  $\Delta$  is the set of  $(a, b) \in K^* \times K^*$  such that for some  $M$  with  $a, b \in M$ ,  $S_M(a, b)$  contains a prime  $\mathfrak{p}$  with  $\mathfrak{p} | 2$  and  $\nu_{\mathfrak{p}}(-ab) = 2$ . Such  $a$  and  $b$  exist, for example, let  $a = 2$  and  $b = 10$ .

Let  $M \in \mathcal{F}$  and  $(2) = \mathfrak{p}_1 \cdots \mathfrak{p}_k$  in  $M$ . Put  $P_M = \bigcap_i ((1 + \mathfrak{p}_i) \cup \mathfrak{p}_i)$ . Then  $P_M$  is a subring of  $\mathfrak{o}_M$  containing 1. Let  $P_K = \bigcup \{P_M : M \in \mathcal{F}\}$ .  $P_K$  is a subring of  $\mathfrak{O}_K$  containing 1.

**Theorem 19**  $\psi(K) = P_K$ .

The proof is similar to that of Proposition 20 in [1].

**Example 20** 1.  $K_l = \bigcup_n \mathbb{Q}(\cos(2\pi/l^n))$  with  $l$  a prime and with  $l \equiv -1 \pmod{4}$ .

2.  $K_W = \prod_{l \in W} K_l$ . ( $W = \{l \text{ a prime} : l \equiv -1 \pmod{4}\}$ )

3.  $K_0 = \mathbb{Q}(\{\cos(2\pi/l) : l \text{ a prime, } l \equiv -1 \pmod{4}\})$ .

## 5 Undecidability results

Let  $K_l = \bigcup_n \mathbb{Q}(\cos(2\pi/l^n))$ . In [1] we proved that if  $l$  is a prime such that  $l \equiv -1 \pmod{4}$  and 2 is a prime of  $\mathfrak{O}_{K_l}$ , then  $K_l$  is undecidable. But in 2000 C.R. Videla [12] proved that  $K_l$  is undecidable for every prime  $l$ . He considered  $K/F$  a pro- $p$  Galois extension over a number field  $F$  and using Rumely's formula in [6] he proved that  $\mathfrak{O}_{K_l}$  is definable with parameters. Then he also used the results of Kronecker and J. Robinson.

Kronecker [3] determined all sets of conjugate algebraic integers in the interval  $c - 2 \leq x \leq c + 2$ , provided that  $c$  is a rational integer; they have the form

$$x = c + 2 \cos(2k\pi/m) \text{ with } 0 \leq k \leq m/2 \text{ and } (k, m) = 1.$$

Note that if  $m = 1, 2, 3, 4$ , then  $x = c + 2, c - 2, c \pm 1, c$  respectively. Furthermore it is known that an interval of length less than 4 can contain only finitely many complete sets of conjugate algebraic integers. (See [11].)

Therefore we see that the interval  $(0, 4)$  contains infinitely many complete conjugate sets of totally real algebraic integers and that no sub-interval does.

These facts are used by J. Robinson in [9]. Her results concerns the integral closure of  $\mathbb{Z}$  inside totally real fields, not necessarily finite over  $\mathbb{Q}$ . She calls such a ring a totally real algebraic integer ring. In 1962 she proved the following: The natural numbers can be defined arithmetically in any totally real algebraic integer ring  $A$  such that there is a smallest interval  $(0, s)$  with  $s$  real or  $\infty$ , which contains infinitely many complete conjugate sets of numbers of  $A$ . But we can say more. We recall that  $\mathbb{Z}^{tr}$  denotes the ring of all totally real algebraic integers.

**Theorem 21** *Let  $R$  be a subring of  $\mathbb{Z}^{tr}$  containing  $\mathbb{Z}$  such that there is a smallest interval  $(0, s)$  with  $s$  real or  $\infty$ , which contains infinitely many complete conjugate sets of numbers of  $R$ . Here  $s$  need not be in  $R$ . Then  $\mathbb{N}$  is definable in  $R$ .*

*In particular such a ring is undecidable.*

The proof of J. Robinson just works. See [9, pp. 300–301].

Thus it follows that for every positive integer  $l > 1$ ,  $\mathfrak{O}_{K_l}$  is undecidable, from which Videla proved that  $K_l$  is undecidable. Note that even if the defining formula contains parameters it is possible to define  $\mathbb{N}$ . See [12].

We give alternative proof of this fact in the case where  $l$  is a prime with  $l \equiv -1 \pmod{4}$ . We know that  $\psi(K_l)$  is a subring of  $\mathbb{Z}^{tr}$  containing  $\mathbb{Z}$  if  $l$  is a prime such that  $l \equiv -1 \pmod{4}$ . Furthermore we know by [11, p. 312], that  $2 + 2\cos(2\pi/l^n)$  are units in  $\mathfrak{O}_{K_l}$  and that  $1 + 2\cos(2\pi/l^n)$  are units in  $\mathfrak{O}_{K_l}$  if  $l \neq 3$ , and  $|N_{F_n/\mathbb{Q}}(1 + 2\cos(2\pi/3^n))| = 3$  for  $n \geq 2$ . Hence we see that  $2 + 2\cos(2\pi/l^n)$  are not in  $\psi(K_l)$  if  $l^n \neq 3$ . On the other hand  $4 + 4\cos(2\pi/l^n)$  are in  $\bigcap_i \mathfrak{P}_i^{(2)}$ , hence in  $\psi(K_l)$ . Thus we see that the interval  $(0, 8)$  contains infinitely many complete conjugate sets of numbers of  $\psi(K_l)$  and the interval  $(0, 4)$  does not. We show that  $(0, 8)$  is actually such a smallest interval for  $\psi(K_l)$ .

**Lemma 22** *Let  $l$  be an odd prime such that  $l \equiv -1 \pmod{4}$ . Then  $(0, 8)$  is a smallest interval of the form  $(0, c)$  which contains infinitely many complete conjugate sets of numbers of  $\psi(K_l)$ .*

*Proof.* We know that  $K_l$  has only finitely many primes lying above 2. (See Lemma 13 in [1].) Thus  $\psi(K_l) = P_{K_l} = \bigcap_i ((1 + \mathfrak{P}_i) \cup \mathfrak{P}_i)$ , where  $\mathfrak{P}_1, \dots, \mathfrak{P}_k$  are primes of  $K_l$  lying above 2. We easily see that  $\psi(K_l)$  is a union of  $2^k$  cosets of  $\mathfrak{O}_{K_l}/2\mathfrak{O}_{K_l}$ .

Suppose that  $(0, 8)$  is not such a smallest interval. Then some interval  $(0, \delta)$  with  $\delta < 8$  contains infinitely many complete conjugate sets of numbers of  $\psi(K_l)$ . Then we have that some coset, say  $\alpha + 2\mathfrak{O}_{K_l}$ , contains infinitely many complete conjugate

sets of numbers. It follows that an interval of length less than 4 contains infinitely many complete conjugate sets of algebraic integers, a contradiction.  $\square$

Let  $K_\Delta = \prod_{l \in \Delta} K_l$  where  $\Delta$  is a finite set of primes. From the result of Videla we deduce that  $K_\Delta$  is undecidable. If  $\Delta$  is a finite set of primes with  $l \equiv -1 \pmod{4}$ , then we can give another proof similarly.

Nevertheless we can give a new undecidable infinite algebraic extension of  $\mathbb{Q}$  by our method. Let  $V$  be a set of Sophie Germain primes, that is, a prime  $p$  such that  $2p + 1$  is again a prime. It is considered that there are infinitely many Sophie Germain primes but it is not proved. Let  $K_V = \mathbb{Q}(\{\cos(2\pi/l) : l \in V\})$ . Then we have  $\psi(K_V) = (1 + 2\mathfrak{O}_{K_V}) \cup \mathfrak{O}_{K_V}$ , hence  $K_V$  is undecidable.

## References

- [1] K. Fukuzaki, Undecidable infinite totally real extensions of  $\mathbb{Q}$ , Kokyuroku of RIMS, 1602 (2008), pp. 37–62.
- [2] S. Iyanaga(Editor), The Theory of Numbers, North-Holland Publishing Company, 1975.
- [3] L. Kronecker, Zwei Sätze über Gleichungen mit ganzzahligen Coefficienten, Reine. Angew. Math., 53 (1857), pp. 173–175.
- [4] S. Lang, Algebraic Number Theory, 2nd ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 1994.
- [5] R. Lidl, H. Niederreiter, Finite fields, Encyclopedia of Mathematics and its Applications, vol. 20, Cambridge University Press, 1997.
- [6] R. Rumely, The undecidability of algebraic rings and fields, Proc. Amer. Math. Soc., 262 (1980), pp 195–217.
- [7] O.T. O'Meara, Introduction to Quadratic Forms, Springer-Verlag, Berlin Heidelberg New York, 1973.
- [8] J. Robinson, The undecidability of algebraic rings and fields, Proc. Amer. Math. Soc., 10 (1959), pp. 950–957.
- [9] J. Robinson, On the decision problem for algebraic rings, Studies in Mathematical Analysis and Related Topics, no. 42, Stanford Univ. Press, Stanford, Calif., 1962, pp. 297–304.
- [10] J. Robinson, The decision problem for fields, The Theory of Models: Proceedings of the 1963 International Symposium at Berkeley (J. W. Addison et al., eds.), North-Holland, Amsterdam, 1965, pp. 299–311.

- [11] R.M. Robinson, Intervals Containing Infinitely Many Sets of Conjugate Algebraic Integers, *Studies in Mathematical Analysis and Related Topics*, no. 43, Stanford Univ. Press, Stanford, Calif., 1962, pp. 305–315.
- [12] C.R. Videla, Definability of the ring of integers in pro- $p$  Galois extensions of number fields, *Israel J. Math.*, 118 (2000), pp. 1–14.